Noname manuscript No.
(will be inserted by the editor)

2- and 3-modular Lattice Wiretap Codes in Small Dimensions

Fuchun Lin · Frédérique Oggier · Patrick Solé

Received: date / Accepted: date

Abstract A recent line of work on lattice codes for Gaussian wiretap channels introduced a new lattice invariant called secrecy gain as a code design criterion which captures the confusion that lattice coding produces at an eavesdropper. Following up the study of unimodular lattice wiretap codes [1], this paper investigates 2- and 3-modular lattices and compares them with unimodular lattices. Most even 2- and 3-modular lattices are found to have better performance (that is, a higher secrecy gain) than the best unimodular lattices in dimension n, $2 \leq n \leq 23$. Odd 2-modular lattices are considered, too, and three lattices are found to outperform the best unimodular lattices.

Keywords Wiretap codes · Gaussian channel · Lattice codes · Secrecy gain · Modular lattices · Theta series

1 Introduction

In his seminal work, Wyner introduced the wiretap channel [2], a discrete memoryless channel where the sender Alice transmits confidential messages to a legitimate receiver Bob, in the presence of an eavesdropper Eve, who has only partial access to what Bob sees. Both reliable and confidential communication between Alice and Bob is shown to be achievable at the same time, by exploiting the physical difference between the channel to Bob and that to Eve, without the use of cryptographic means. Since then, many results of information theoretical nature have been found for various classes of wiretap channels

Fuchun Lin and Frédérique Oggier
Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, Singapore 637371
E-mail: linf0007@e.ntu.edu.sg and frederique@ntu.edu.sg

Patrick Solé
Telecom ParisTech, CNRS, UMR 5141, Dept Comelec, 46 rue Barrault 75634 Paris cedex 13, France and Mathematics Department, King AbdulAziz Unversity, Jeddah, Saudi Arabia.
E-mail: patrick.sole@telecom-paristech.fr

ranging from Gaussian point-to-point channels to relay networks (see e.g. [3] for a survey) capturing the trade-off between reliability and secrecy and aiming at determining the highest information rate that can be achieved with perfect secrecy, the so-called *secrecy capacity*. Coding results focusing on constructing concrete codes that can be implemented in a specific channel are much fewer (see [4,5] for wiretap codes dealing with channels with erasures, [6] for Polar wiretap codes and [7] for wiretap Rayleigh fading channels.

In this paper, we will focus on Gaussian wiretap channels, whose secrecy capacity was established in [8]. Examples of existing Gaussian wiretap codes were designed for binary inputs, as in [9,10]. A different approach was adopted in [11], where lattice codes were proposed, using as design criterion a new lattice invariant called *secrecy gain*, defined as the maximum of its *secrecy function* (Section II), which was shown to characterize the confusion at the eavesdropper. A recent study on a new design criterion called *flatness factor* confirms that to confuse Eve, the secrecy gain should be maximized [12]. This suggests the study of the secrecy gain of lattices as a way to understand how to design a good Gaussian lattice wiretap code. Belfiore and Solé [13] discovered a symmetry point, called *weak secrecy gain*, in the secrecy function of *unimodular* lattices (generalized to all ℓ*-modular* lattices [14]) and conjectured that the weak secrecy gain is actually the secrecy gain. Anne-Maria Ernvall-Hytönen [15,16] invented a method to prove or disprove the conjecture for unimodular lattices. Up to date, secrecy gains of a special class of unimodular lattices called *extremal unimodular* lattices and all unimodular lattices in dimensions up to 23 are computed [14,1]. The asymptotic behavior of the average weak secrecy gain as a function of the dimension n was investigated and an achievable lower bound on the secrecy gain of even unimodular lattices was given [14]. Numerical upper bounds on the secrecy gains of unimodular lattices in general and unimodular lattices constructed from self-dual binary codes were given to compared with the achievable lower bound [17].

This paper studies the weak secrecy gain of 2- and 3-modular lattices. Preliminary work [18] showed that most of the known even 2- and 3-modular lattices in dimensions up to 24 have secrecy gains bigger than the best unimodular lattices. After recalling how to compute the weak secrecy gain of even 2- and 3-modular lattices using the theory of modular forms, we extend our study to a class of odd 2-modular lattices constructed from self-dual codes. We propose two methods to compute their weak secrecy gains and find three of these lattices have secrecy gains bigger than the best unimodular lattices. We then conclude that, at least in dimensions up to 23, 2- and 3-modular lattices are a better option than unimodular lattices.

The remainder of this paper is organized as follows. In Section 2, we first give a brief introduction to modular lattices and their *theta series* as well as recall the definition of the secrecy gain and the previous results concerning this lattice invariant. The main results are given in Section 3. Two approaches to compute the theta series of modular lattices are given, one making use of the modular form theory while the other utilizing the connection between the theta series and the weight enumerator of self-dual codes. Weak secrecy gains

of several 2- and 3-modular lattices computed are then compared with the best unimodular lattices in Section 4. In Section 5, we summarize our results and give some future works.

2 Preliminaries and previous results

Consider a Gaussian wiretap channel, which is modeled as follows: Alice wants to send data to Bob over a Gaussian channel whose noise variance is given by σ_b^2. Eve is the eavesdropper trying to intercept data through another Gaussian channel with noise variance σ_e^2, where $\sigma_b^2 < \sigma_e^2$, in order to have a positive secrecy capacity [8]. More precisely, the model is

$$\begin{aligned} \mathbf{y} &= \mathbf{x} + \mathbf{v_b} \\ \mathbf{z} &= \mathbf{x} + \mathbf{v_e}. \end{aligned} \tag{1}$$

$\mathbf{x} \in \mathbb{R}^n$ is the transmitted signal. $\mathbf{y}$ and $\mathbf{z}$ are the received signals at Bob's, respectively Eve's side. $\mathbf{v_b}$ and $\mathbf{v_e}$ denote the Gaussian noise vectors at Bob's, respectively Eve's side, each component of both vectors are with zero mean, and respective variance σ_b^2 and σ_e^2. In this paper, we choose $\mathbf{x}$ to be a codeword coming from a specially designed lattice of dimension n, namely, we consider lattice coding. Let us thus start by recalling some concepts concerning lattices, in particular, *modular lattices*.

A *lattice* Λ is an additive subgroup of $\mathbb{R}^n$, which can be described in terms of its *generator matrix* M by

$$\Lambda = \{\mathbf{x} = \mathbf{u}M | \mathbf{u} \in \mathbb{Z}^m\},$$

where

$$M = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \cdots & & \cdots & \\ v_{m1} & v_{m2} & \cdots & v_{mn} \end{pmatrix}$$

and the row vectors $\mathbf{v}_i = (v_{i1}, \cdots, v_{in}),\ i = 1,\ 2,\ \cdots,\ m$ form a basis of the lattice Λ. The matrix

$$G = MM^T,$$

where M^T denotes the transpose of M, is called the *Gram matrix* of the lattice. It is easy to see that the (i, j)th entry of G is the inner product of the ith and jth row vectors of M, denoted by

$$G_{(i,j)} = \mathbf{v}_i \cdot \mathbf{v}_j.$$

The *determinant* $\det(\Lambda)$ of a lattice Λ is the determinant of the matrix G, which is independent of the choice of the matrix M. A *fundamental region* for a lattice is a building block which when repeated many times fills the whole space with just one lattice point in each copy. There are many different ways of choosing a fundamental region for a lattice Λ, but the volume of the

fundamental region is uniquely determined and called the *volume* $\mathrm{vol}(\Lambda)$ of Λ, which is exactly $\sqrt{\det(\Lambda)}$. Let us see an example of a fundamental region of a lattice. A *Voronoi cell* $\mathcal{V}_\Lambda(\mathbf{x})$ of a lattice point $\mathbf{x}$ in Λ consists of the points in the space that are closer to $\mathbf{x}$ than to any other lattice points of Λ.

The *dual* of a lattice Λ of dimension n is defined to be

$$\Lambda^* = \{\mathbf{x} \in \mathbb{R}^n : \mathbf{x} \cdot \lambda \in \mathbb{Z}, \text{ for all } \lambda \in \Lambda\}.$$

A lattice Λ is called an *integral lattice* if $\Lambda \subset \Lambda^*$. The norm of any lattice point in an integral lattice Λ is always an integer. If the norm is even for any lattice point, then Λ is called an *even* lattice. Otherwise, it is called an *odd* lattice. A lattice is said to be *equivalent*, or geometrically similar to its dual, if it differs from its dual only by possibly a rotation, reflection and change of scale. An integral lattice that is equivalent to its dual is called a *modular* lattice. Alternatively as it was first defined by H.-G. Quebbemann [19], an n-dimensional integral lattice Λ is modular if there exists a similarity σ of $\mathbb{R}^n$ such that $\sigma(\Lambda^*) = \Lambda$. If σ multiplies norms by ℓ, Λ is said to be *ℓ-modular*. The determinant of an ℓ-modular lattice Λ of dimension n is given by

$$\det(\Lambda) = \ell^{\frac{n}{2}}. \tag{2}$$

This is because, on the one hand, $\det(\Lambda^*) = \det(\Lambda)^{-1}$ by definition and, on the other hand, $\ell^n \det(\Lambda^*) = \det(\Lambda)$ since $\sigma(\Lambda^*) = \Lambda$. When $\ell = 1$, $\det(\Lambda) = 1$ and we recover the definition of unimodular lattice as an integral lattice whose determinant is 1.

Example 1

$$C^\ell = \sum_{d|\ell} \sqrt{d}\mathbb{Z}, \ \ell = 1, 2, 3, 5, 6, 7, 11, 14, 15, 23 \tag{3}$$

is an ℓ-modular lattice [20]. When ℓ is a prime number, $C^\ell = \mathbb{Z} \oplus \sqrt{\ell}\mathbb{Z}$ is a two-dimensional ℓ-modular lattice with the similarity map σ taking (x, y) to $(\sqrt{\ell}y, \sqrt{\ell}x)$.

We will use some terminology from classical error correction codes in this paper. Unfamiliar readers can refer to [21]. We will also assume basic knowledge of algebraic number theory [22]. There is a classical way of constructing ℓ-modular lattices from self-dual codes called Construction A. Let $K = \mathbb{Q}(\sqrt{\mu})$ be a quadratic imaginary extension of the rational field $\mathbb{Q}$ constructed by adjoining to it the square root of a square free negative integer μ. The ring of integers $\mathfrak{O}_K$ of K is given by

$$\mathfrak{O}_K = \mathbb{Z}[\theta], \ \theta = \begin{cases} \frac{1+\sqrt{\mu}}{2}, & \mu \equiv 1 \pmod 4 \\ \sqrt{\mu}, & \text{otherwise.} \end{cases} \tag{4}$$

Let p be a prime number. Then the quotient ring $R = \mathfrak{O}_K / p\mathfrak{O}_K$ is given by

$$R = \begin{cases} \mathbb{F}_p \times \mathbb{F}_p, & p \text{ is split in } K; \\ \mathbb{F}_p + u\mathbb{F}_p \text{ with } u^2 = 0, & p \text{ is ramified in } K; \\ \mathbb{F}_{p^2}, & p \text{ is inert in } K. \end{cases} \tag{5}$$

Let k be a positive integer. Let

$$\rho : \mathfrak{O}_K^k \to R^k$$

be the map of component wise reduction modulo $p\mathfrak{O}_K$. Then the pre-image $\rho^{-1}(C)$ of a self-dual code C over R of length k with carefully chosen μ and p and possibly a re-scaling can give rise to a real ℓ-modular lattice of dimension $2k$ [23,24]. Examples will be specified in the sequel.

Definition 1 The theta series of a lattice Λ is defined by

$$\Theta_\Lambda(\tau) = \Sigma_{\lambda\in\Lambda} q^{||\lambda||^2}, q = e^{\pi i\tau},\ \tau \in \mathcal{H},$$

where $||\lambda||^2 = \lambda\cdot\lambda$ is called the (squared) norm of λ and $\mathcal{H} = \{a+ib \in \mathbb{C} | b > 0\}$ denotes the upper half plane.

The theta series of an integral lattice has a neat representation. Since the norms are all integers, we can combine the terms with the same norm and write

$$\Theta_\Lambda(\tau) = \Sigma_{m=0}^{\infty} A_m q^m, \tag{6}$$

where A_m counts the number of lattice points with norm m. They are actually *modular forms* [25].

We will also need the following functions and formulae from analytic number theory for our discussion, for which interested readers can refer to [26].

Definition 2 The Jacobi theta functions are defined as follows:

$$\begin{cases} \vartheta_2(\tau) = \Sigma_{m\in\mathbb{Z}} q^{(m+\frac{1}{2})^2}, \\ \vartheta_3(\tau) = \Sigma_{m\in\mathbb{Z}} q^{m^2}, \\ \vartheta_4(\tau) = \Sigma_{m\in\mathbb{Z}} (-q)^{m^2}. \end{cases}$$

Definition 3 The Dedekind eta function is defined by

$$\eta(\tau) = q^{\frac{1}{12}} \prod_{m=1}^{\infty} (1-q^{2m}).$$

The Jacobi theta functions and the Dedekind eta function are connected as follows [26]:

$$\begin{cases} \vartheta_2(\tau) = \frac{2\eta(2\tau)^2}{\eta(\tau)}, \\ \vartheta_3(\tau) = \frac{\eta(\tau)^5}{\eta(\frac{\tau}{2})^2\eta(2\tau)^2}, \\ \vartheta_4(\tau) = \frac{\eta(\frac{\tau}{2})^2}{\eta(\tau)}. \end{cases} \tag{7}$$

Lattice encoding for the wiretap channel (1) is done via a generic coset coding strategy [11]: let $\Lambda_e \subset \Lambda_b$ be two nested lattices. A k-bit message is mapped to a coset in Λ_b/Λ_e, after which a vector is randomly chosen from the coset as the encoded word. The lattice Λ_e can be interpreted as introducing confusion for Eve, while Λ_b is intended to ensure reliability for Bob. Since a

message is now corresponding to a coset of codewords instead of one single codeword, the probability of correct decoding is then summing over the whole coset (suppose that we do not have power constraint and are utilizing the whole lattice to do the encoding). Here we are interested in computing $P_{c,e}$, Eve's probability of correct decision, and want to minimize this probability. It was shown in [11,14] that to minimize $P_{c,e}$ is to minimize

$$\sum_{\mathbf{t}\in\Lambda_e} e^{-||\mathbf{t}||^2/2\sigma_e^2}, \tag{8}$$

which is easily recognized as the theta series of Λ_e at $\tau = \frac{i}{2\pi\sigma_e^2}$. We hence only care about values of τ such that $\tau = yi,\ y > 0$.

Motivated by the above argument, the confusion brought by the lattice Λ_e with respect to no coding (namely, use a scaled version of the lattice $\mathbb{Z}^n$ with the same volume) is measured as follows:

Definition 4 [11] Let Λ be an n-dimensional lattice of volume v^n. The secrecy function of Λ is given by

$$\Xi_\Lambda(\tau) = \frac{\Theta_{v\mathbb{Z}^n}(\tau)}{\Theta_\Lambda(\tau)}, \tau = yi, y > 0.$$

The *secrecy gain* is then the maximal value of the secrecy function with respect to τ and is denoted by χ_Λ.

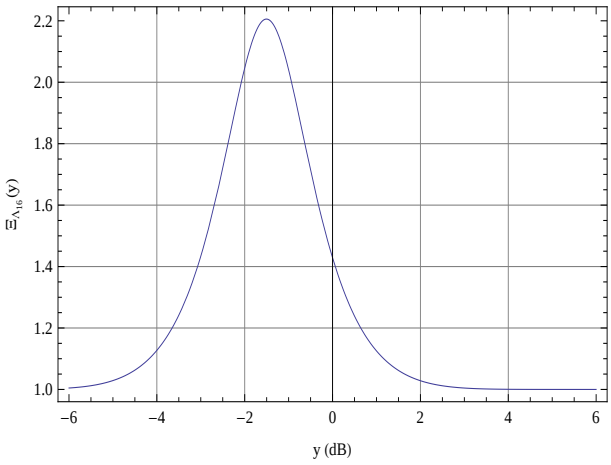

Fig. 1 Secrecy function of BW_{16}

ℓ-modular lattices were shown to have a symmetry point, called *weak secrecy gain* χ_Λ^w, at $\tau = \frac{i}{\sqrt{\ell}}$ in their secrecy function [14]. See Fig. 1 for an example, where y is plotted in dB to transform the multiplicative symmetry point into an additive symmetry point. BW_{16} is a 2-modular lattice. One can

see there is a symmetry point at $y = -\frac{3}{2}$ dB, which is $\frac{\sqrt{2}}{2}$. This paper is devoted to computing the weak secrecy gain of 2- and 3-modular lattices in small dimensions.

3 The weak secrecy gain of 2- and 3-modular lattices in small dimensions

The key to the computation of secrecy gains is the theta series of the corresponding lattice. We present here two approaches to obtain a closed form expression of the theta series of 2- and 3-modular lattices: the modular form approach and the weight enumerator approach. The modular form approach relies on the fact that the theta series of an ℓ-modular lattice belongs to the space of modular forms generated by some basic functions, which gives a decomposition formula. The formula for even 2- and 3-modular lattices is comparatively simple while the formula for ℓ-modular lattices in general, including the odd lattices, is rather complicated. A weight enumerator approach is added in the computation for odd 2-modular lattices in the second subsection. This approach exploits the connection between the weight enumerator of a self-dual code and the theta series of a lattice constructed from this code. But calculating the weight enumerator of the code adds considerable workload.

3.1 Even 2 and 3-modular lattices

The theta series of modular lattices are modular forms, which, roughly speaking, are functions that stay "invariant" under the transformation by certain subgroups of the group $\mathrm{SL}_2(\mathbb{Z})$ [25]. The modular form theory shows that theta series as modular forms are expressed in a polynomial in two basic modular forms. We only need a few terms of a theta series to compute the coefficients of this expression and obtain a closed form expression of the theta series. The following lemma plays a crucial role in our calculation of the theta series of 2- and 3-modular lattices.

Lemma 1 *[19] The theta series of an even ℓ-modular lattice of dimension $n = 2k$ when $\ell = 1,\ 2,\ 3$ belongs to a space of modular forms of weight k generated by the functions $\Theta_{2k_0}^{\lambda}(\tau)\Delta_{2k_1}^{\mu}(\tau)$ with integers $\lambda,\ \mu \geq 0$ satisfying $k_0\lambda + k_1\mu = k$, where for $\ell = 1,\ 2,\ 3$, $k_0 = 4,\ 2,\ 1$ respectively, $k_1 = \frac{24}{1+\ell}$, $\Theta_{2k_0}(\tau)$ denote the theta series of the modular lattices E_8, D_4 and A_2, respectively, and $\Delta_{2k_1}(\tau) = (\eta(\tau)\eta(\ell\tau))^{k_1}$.*

Example 2 If $\ell = 1$, we read from Lemma 1 that $k_0 = 4$, $k_1 = \frac{24}{2} = 12$, $\Theta_{2k_0}(\tau) = \Theta_{E_8}(\tau)$ and $\Delta_{2k_1}(\tau) = \eta^{24}(\tau)$. We then deduce that if Λ is an even unimodular lattice of dimension $n = 2k$ then

$$\Theta_{\Lambda}(\tau) = \sum_{4\lambda+12\mu=k} a_{\mu}\Theta_{E_8}^{\lambda}(\tau)\Delta_{24}^{\mu}(\tau). \tag{9}$$

The formula (9) was adopted in [13,14] to compute the secrecy gains of several even unimodular lattices.

In order to write the secrecy function, we need to have the theta series of $\mathbb{Z}^n$ scaled to the right volume. Now it follows from (2) that

$$\Theta_{\ell^{\frac{1}{4}}\mathbb{Z}^n}(\tau) = \vartheta_3^n(\sqrt{\ell}\tau). \tag{10}$$

According to Lemma 1, the theta series of an even 2-modular lattice Λ of dimension $n = 2k$ can be written as

$$\Theta_\Lambda(\tau) = \sum_{2\lambda+8\mu=k} a_\mu \Theta_{D_4}^\lambda(\tau)\Delta_{16}^\mu(\tau), \tag{11}$$

where

$$\begin{aligned}\Theta_{D_4}(\tau) &= \tfrac{1}{2}\left(\vartheta_3^4(\tau) + \vartheta_4^4(\tau)\right)\\ &= 1 + 24q^2 + 24q^4 + 96q^6 + \cdots\end{aligned} \tag{12}$$

and

$$\Delta_{16}(\tau) = \left(\eta(\tau)\eta(2\tau)\right)^8.$$

By (7), we can write $\Delta_{16}(\tau)$ in terms of Jacobi theta functions and compute the first few terms:

$$\begin{aligned}\Delta_{16}(\tau) &= \tfrac{1}{2^{56}}\vartheta_2^8(\tau)\vartheta_3^4(\tau)\vartheta_4^4(\tau)\\ &= q^2 - 8q^4 + 12q^6 + \cdots.\end{aligned} \tag{13}$$

The secrecy function of an even 2-modular lattice Λ of dimension n is then written as

$$\Xi_\Lambda(\tau) = \frac{\vartheta_3^n(\sqrt{2}\tau)}{\sum_{2\lambda+8\mu=k} a_\mu \Theta_{D_4}^\lambda(\tau)\Delta_{16}^\mu(\tau)},$$

or more conveniently,

$$\begin{aligned}1/\Xi_\Lambda(\tau) &= \textstyle\sum_{2\lambda+8\mu=k} a_\mu \frac{\Theta_{D_4}^\lambda(\tau)\Delta_{16}^\mu(\tau)}{\vartheta_3^n(\sqrt{2}\tau)}\\ &= \textstyle\sum_{2\lambda+8\mu=k} a_\mu \left(\frac{\Theta_{D_4}(\tau)}{\vartheta_3^4(\sqrt{2}\tau)}\right)^\lambda \left(\frac{\Delta_{16}(\tau)}{\vartheta_3^{16}(\sqrt{2}\tau)}\right)^\mu.\end{aligned}$$

Now we only need to know the coefficients a_μ in order to compute the weak secrecy gain of a 2-modular lattice.

Let us compute an example to show how the coefficients a_μ's in (11) are computed. By substituting (12) and (13) into (11), we have a formal sum with coefficients represented by the a_μ's. Then by comparing this formal sum with (6), we obtain a number of linear equations in the a_μ's. When we have enough equations, the a_μ's can be recovered by solving a linear system.

Example 3 BW_{16} is an even lattice with minimum norm 4. The theta series of BW_{16} looks like

$$\Theta_{BW_{16}}(\tau) = 1 + 0q^2 + A_4q^4 + \cdots,\ A_4 \neq 0.$$

On the other hand, by (11), (12) and (13),

$$\begin{aligned}\Theta_{BW_{16}}(\tau) &= a_0\Theta_{D_4}^4(\tau) + a_1\Delta_{16}(\tau)\\ &= a_0(1+24q^2+\cdots)^4 + a_1(q^2+\cdots)\\ &= a_0(1+96q^2+\cdots) + a_1(q^2+\cdots)\\ &= a_0 + (96a_0+a_1)q^2+\cdots.\end{aligned}$$

We now have two linear equations in two unknowns a_0 and a_1

$$\begin{cases} a_0 = 1\\ 96a_0 + a_1 = 0\end{cases}$$

which gives $a_0 = 1$ and $a_1 = -96$, yielding the theta series

$$\Theta_{BW_{16}} = \Theta_{D_4}^4 - 96\Delta_{16}. \tag{14}$$

The weak secrecy gain of BW_{16} can then be approximated using Mathematica [27] (see Fig. 1):

$$\chi_{BW_{16}} = 2.20564. \tag{15}$$

Similarly according to Lemma 1, the theta series of an even 3-modular lattice Λ of dimension $n = 2k$ can be written as

$$\Theta_\Lambda(\tau) = \sum_{\lambda+6\mu=k} a_\mu \Theta_{A_2}^\lambda(\tau)\Delta_{12}^\mu(\tau), \tag{16}$$

where

$$\begin{aligned}\Theta_{A_2}(\tau) &= \vartheta_2(2\tau)\vartheta_2(6\tau) + \vartheta_3(2\tau)\vartheta_3(6\tau)\\ &= 1 + 6q^2 + 0q^4 + 6q^6 + \cdots\end{aligned} \tag{17}$$

and

$$\Delta_{12}(\tau) = (\eta(\tau)\eta(3\tau))^6.$$

We can also compute the first few terms of $\Delta_{12}(\tau)$:

$$\Delta_{12}(\tau) = q^2 - 6q^4 + 9q^6 + \cdots. \tag{18}$$

The secrecy function of an even 3-modular lattice Λ of dimension n is

$$\begin{aligned}1/\Xi_\Lambda(\tau) &= \textstyle\sum_{\lambda+6\mu=k} \frac{a_\mu \Theta_{A_2}^\lambda(\tau)\Delta_{12}^\mu(\tau)}{\vartheta_3^n(\sqrt{3}\tau)}.\\ &= \textstyle\sum_{\lambda+6\mu=k} a_\mu \left(\frac{\Theta_{A_2}(\tau)}{\vartheta_3^2(\sqrt{3}\tau)}\right)^\lambda \left(\frac{\Delta_{12}(\tau)}{\vartheta_3^{12}(\sqrt{3}\tau)}\right)^\mu.\end{aligned}$$

Table 1 summarizes the weak secrecy gains of even 2- and 3-modular lattices computed. The basic information about these lattices, such as minimum norm and kissing number can be found in [28].

Table 1 Weak secrecy gains of the known even 2- and 3-modular lattices

dim	lattice	ℓ	theta series	$\chi_{\mathcal{A}}^{w}$
2	A_2	3	Θ_{A_2}	1.01789
4	D_4	2	Θ_{D_4}	1.08356
12	K_{12}	3	$\Theta_{A_2}^6 - 36\Delta_{12}$	1.66839
14	$C^2 \times G(2,3)$	3	$\Theta_{A_2}^7 - 42\Theta_{A_2}\Delta_{12}$	1.85262
16	BW_{16}	2	$\Theta_{D_4}^4 - 96\Delta_{16}$	2.20564
20	HS_{20}	2	$\Theta_{D_4}^5 - 120\Theta_{D_4}\Delta_{16}$	3.03551
22	$A_2 \times A_{11}$	3	$\Theta_{A_2}^{11} - 66\Theta_{A_2}^5\Delta_{12}$	3.12527
24	$L_{24.2}$	3	$\Theta_{A_2}^{12} - 72\Theta_{A_2}^6\Delta_{12} - 216\Delta_{12}^2$	3.92969

3.2 Odd 2-modular lattices

Odd 2-modular lattices were constructed in [23,24] via Construction A. They are, by the time of writing this paper, the only known instances of odd 2-modular lattices. There is a natural connection between the theta series of the lattice constructed from a code C via Construction A and an appropriate weight enumerator of the code C. We will exploit this connection to obtain a closed form expression for these lattices.

For the rest of the paper, we will let $K = \mathbb{Q}(\sqrt{-2})$ and $R = \mathfrak{O}_K/3\mathfrak{O}_K$, where the notations are explained in Section 2. According to (4), since $-2 \equiv 2 \bmod 4$, the ring of integers $\mathfrak{O}_K$ of K is $\mathfrak{O}_K = \mathbb{Z}[\sqrt{-2}] = \{a+b\sqrt{-2} | a, b \in \mathbb{Z}\}$. Now we consider the decomposition of the prime ideal $3\mathfrak{O}_K$. Since $3 = (1+\sqrt{-2})(1-\sqrt{-2})$ and $(1+\sqrt{-2})\mathfrak{O}_K \neq (1-\sqrt{-2})\mathfrak{O}_K$, the ideal $3\mathfrak{O}_K$ splits. According to (5), the quotient ring $R = \mathfrak{O}_K/3\mathfrak{O}_K = \mathbb{F}_3 \times \mathbb{F}_3$. Note that the ring $\mathbb{F}_3 + v\mathbb{F}_3$ with $v^2 = 1$ is isomorphic to the ring $\mathbb{F}_3 \times \mathbb{F}_3$, through an isomorphism $\delta:\ a(v-1) + b(v+1) \mapsto (a, b)$. We will identify $R = \mathfrak{O}_K/3\mathfrak{O}_K$ with the ring $\mathbb{F}_3 + v\mathbb{F}_3$ and use the two notations interchangeably. In particular, we will identify the coset $a + 3\mathfrak{O}_K$ with $a \in \mathbb{F}_3$, and the coset $\sqrt{-2} + 3\mathfrak{O}_K$ with v.

Let C be a code of length $n = 2k$ over $R = \mathbb{F}_3 + v\mathbb{F}_3 = \mathfrak{O}_K/3\mathfrak{O}_K$, which is by definition a R-submodule of R^n. According to Construction A, $\rho^{-1}(C)$ is a lattice over $\mathfrak{O}_K$[1], say, with generator matrix

$$\begin{pmatrix} \lambda_{11} & \cdots & \lambda_{1k} \\ & \cdots & \\ \lambda_{k1} & \cdots & \lambda_{kk} \end{pmatrix}.$$

[1] A k-dimensional lattice can be defined in a more general setting by a free abelian group of rank k.

Let $\frac{1}{\sqrt{3}}\rho^{-1}(C)_{real}$ denote the real lattice defined by the generator matrix

$$\frac{1}{\sqrt{3}}\begin{pmatrix} \mathrm{Re}(\lambda_{11})\ \mathrm{Im}(\lambda_{11}) & \cdots & \mathrm{Re}(\lambda_{1k})\ \mathrm{Im}(\lambda_{1k}) \\ \mathrm{Im}(\lambda_{11})\ \mathrm{Re}(\lambda_{11}) & \cdots & \mathrm{Im}(\lambda_{1k})\ \mathrm{Re}(\lambda_{1k}) \\ & \cdots & \\ \mathrm{Re}(\lambda_{k1})\ \mathrm{Im}(\lambda_{k1}) & \cdots & \mathrm{Re}(\lambda_{kk})\ \mathrm{Im}(\lambda_{kk}) \\ \mathrm{Im}(\lambda_{k1})\ \mathrm{Re}(\lambda_{k1}) & \cdots & \mathrm{Im}(\lambda_{kk})\ \mathrm{Re}(\lambda_{kk}) \end{pmatrix}.$$

Now we look at the theta series of the lattice $\frac{1}{\sqrt{3}}\rho^{-1}(C)_{real}$ constructed from a code C over R.

Definition 5 [24] The *length function* l_K of an element r in $R = \mathbb{F}_3 + v\mathbb{F}_3 = \mathfrak{O}_K/3\mathfrak{O}_K$ is defined by

$$l_K(r) = \inf\{x\bar{x} | x \in r \subset \mathfrak{O}_K\}, \tag{19}$$

where $\bar{x}$ is the complex conjugation of x.

One computes the length of the nine elements of R as follows:

$$\begin{cases} l_K(0) & = 0 \\ l_K(\pm 1) & = 1 \\ l_K(\pm v) & = 2 \\ l_K(\pm 1 \pm v) & = 3. \end{cases} \tag{20}$$

Definition 6 [24] The *length composition* $n_l(\mathbf{x})$, $l = 0, 1, 2, 3$ of a vector $\mathbf{x}$ in R^n counts the number of coordinates of length l. The *length weight enumerator* of a code C over R is then defined by

$$\mathrm{lwe}_C(a, b, c, d) = \sum_{\mathbf{c} \in C} a^{n_0(\mathbf{c})} b^{n_1(\mathbf{c})} c^{n_2(\mathbf{c})} d^{n_3(\mathbf{c})}. \tag{21}$$

Define four theta series θ_l, $l = 0, 1, 2, 3$ corresponding to the four different lengths of elements of R:

$$\begin{cases} \theta_0 = \sum_{x \in 3\mathfrak{O}_K} q^{\frac{x\bar{x}}{3}} \\ \theta_1 = \sum_{x \in 1+3\mathfrak{O}_K} q^{\frac{x\bar{x}}{3}} \\ \theta_2 = \sum_{x \in \sqrt{-2}+3\mathfrak{O}_K} q^{\frac{x\bar{x}}{3}} \\ \theta_3 = \sum_{x \in 1+\sqrt{-2}+3\mathfrak{O}_K} q^{\frac{x\bar{x}}{3}}. \end{cases} \tag{22}$$

Recalling that $\mathfrak{O}_K = \{a + b\sqrt{-2} | a, b \in \mathbb{Z}\}$, the theta series are written as double sums.

$$\begin{cases} \theta_0 = \sum_{a \in \mathbb{Z}} \sum_{b \in \mathbb{Z}} q^{3a^2+6b^2} \\ \theta_1 = \sum_{a \in \mathbb{Z}} \sum_{b \in \mathbb{Z}} q^{3(a+\frac{1}{3})^2+6b^2} \\ \theta_2 = \sum_{a \in \mathbb{Z}} \sum_{b \in \mathbb{Z}} q^{3a^2+6(b+\frac{1}{3})^2} \\ \theta_3 = \sum_{a \in \mathbb{Z}} \sum_{b \in \mathbb{Z}} q^{3(a+\frac{1}{3})^2+6(b+\frac{1}{3})^2}. \end{cases} \tag{23}$$

We already know how to handle the lm^2 type of infinite sum, namely,

$$\sum_{m\in\mathbb{Z}} q^{lm^2} = \sum_{m\in\mathbb{Z}} (q^l)^{m^2} = \vartheta_3(l\tau).$$

For the $(3m+1)^2$ type of infinite sum, we first observe that, on one hand,

$$\sum_{m\in\mathbb{Z}} q^{m^2} = \sum_{m\in\mathbb{Z}} q^{(3m)^2} + \sum_{m\in\mathbb{Z}} q^{(3m+1)^2} + \sum_{m\in\mathbb{Z}} q^{(3m-1)^2}$$

and, on the other hand,

$$\sum_{m\in\mathbb{Z}} q^{(3m+1)^2} = \sum_{m\in\mathbb{Z}} q^{(3m-1)^2}.$$

We then conclude that

$$\begin{aligned}\textstyle\sum_{m\in\mathbb{Z}} q^{(3m+1)^2} &= \tfrac{1}{2}\left(\textstyle\sum_{m\in\mathbb{Z}} q^{m^2} - \sum_{m\in\mathbb{Z}} q^{(3m)^2}\right)\\ &= \tfrac{1}{2}\left(\vartheta_3(\tau) - \vartheta_3(9\tau)\right).\end{aligned}$$

The four theta series defined above are then computed as

$$\begin{cases}\theta_0 = \vartheta_3(3\tau)\vartheta_3(6\tau)\\ \theta_1 = \frac{1}{2}\left(\vartheta_3(\frac{\tau}{3}) - \vartheta_3(3\tau)\right)\vartheta_3(6\tau)\\ \theta_2 = \frac{1}{2}\vartheta_3(3\tau)\left(\vartheta_3(\frac{2\tau}{3}) - \vartheta_3(6\tau)\right)\\ \theta_3 = \frac{1}{4}\left(\vartheta_3(\frac{\tau}{3}) - \vartheta_3(3\tau)\right)\left(\vartheta_3(\frac{2\tau}{3}) - \vartheta_3(6\tau)\right).\end{cases} \tag{24}$$

Theorem 1

$$\Theta_{\frac{1}{\sqrt{3}}\rho^{-1}(C)}(q) = lwe_C(\theta_0,\theta_1,\theta_2,\theta_3). \tag{25}$$

Proof The theta series of the lattice $\frac{1}{\sqrt{3}}\rho^{-1}(C)$ is by definition

$$\begin{aligned}\Theta_{\frac{1}{\sqrt{3}}\rho^{-1}(C)}(\tau) &= \textstyle\sum_{\lambda\in\frac{1}{\sqrt{3}}\rho^{-1}(C)} q^{||\lambda||^2}\\ &= \textstyle\sum_{\mathbf{c}\in C}\sum_{\mathbf{x}\in\frac{1}{\sqrt{3}}(\mathbf{c}+3\mathfrak{D}_K^k)} q^{\mathbf{x}\bar{\mathbf{x}}}\\ &= \textstyle\sum_{\mathbf{c}\in C}\theta_0^{n_0(\mathbf{c})}\theta_1^{n_1(\mathbf{c})}\theta_2^{n_2(\mathbf{c})}\theta_3^{n_3(\mathbf{c})}\\ &= \mathrm{lwe}_C(\theta_0,\theta_1,\theta_2,\theta_3).\end{aligned}$$

As it was remarked in [23] (Remark 3.8) and later proved in [24], if C is a self-dual code over R with respect to Hermitian inner product, then $\frac{1}{\sqrt{3}}\rho^{-1}(C)_{real}$ is an odd 2-modular lattice.

Example 4 A Hermitian self-dual code C over R of length 4 was constructed in [24]. It is a linear code with a generator matrix

$$G^H = \begin{bmatrix}1 & 0 & v & -1-v\\ 0 & 1 & -1+v & v\end{bmatrix}. \tag{26}$$

One can generate all the 81 codewords and compute the length weight enumerator:

$$\begin{aligned}\mathrm{lwe}_C(a,b,c,d) = {} & a^4 + 4a^2d^2 + 16abcd + 8ad^3 + 8b^3d\\ & +4b^2c^2 + 24bcd^2 + 8c^3d + 8d^4.\end{aligned}$$

The theta series of the 8-dimensional odd 2-modular lattice is then computed by (25) (using a computer software, for example, Mathematica [27] to output the first few terms).

$$\begin{aligned}
&\Theta_{\frac{1}{\sqrt{3}}\rho^{-1}(C)}(\tau)\\
&= \vartheta_3(3\tau)^4\vartheta_3(6\tau)^4\\
&+\tfrac{1}{4}\vartheta_3(3\tau)^3\left(\vartheta_3(\tfrac{\tau}{3})-\vartheta_3(3\tau)\right)\left(\vartheta_3(\tfrac{2\tau}{3})-\vartheta_3(6\tau)\right)^4\\
&+\tfrac{3}{2}\vartheta_3(3\tau)^2\vartheta_3(6\tau)^2\left(\vartheta_3(\tfrac{\tau}{3})-\vartheta_3(3\tau)\right)^2\left(\vartheta_3(\tfrac{2\tau}{3})-\vartheta_3(6\tau)\right)^2\\
&+\tfrac{5}{8}\vartheta_3(3\tau)\vartheta_3(6\tau)\left(\vartheta_3(\tfrac{\tau}{3})-\vartheta_3(3\tau)\right)^3\left(\vartheta_3(\tfrac{2\tau}{3})-\vartheta_3(6\tau)\right)^3\\
&+\tfrac{1}{4}\vartheta_3(6\tau)^3\left(\vartheta_3(\tfrac{\tau}{3})-\vartheta_3(3\tau)\right)^4\left(\vartheta_3(\tfrac{2\tau}{3})-\vartheta_3(6\tau)\right)\\
&+\tfrac{1}{32}\left(\vartheta_3(\tfrac{\tau}{3})-\vartheta_3(3\tau)\right)^4\left(\vartheta_3(\tfrac{2\tau}{3})-\vartheta_3(6\tau)\right)^4\\
&= 1+32q^2+128q^3+240q^4+\cdots.
\end{aligned}$$

This method has the advantage of being self-contained in its deduction. But the computation of the weight enumerator of the code C is tedious and, worse still, as the dimension increases, it may become infeasible. Let us fall back to the first approach adopted in the previous subsection.

First we need a formula similar to Lemma 1 which deals with the theta series of odd 2-modular lattices. There is indeed a formula which deals with the theta series of ℓ-modular lattice, including the odd lattices, for $\ell = 1, 2, 3, 5, 6, 7, 11, 14, 15, 23$ discovered by E. M. Rains and N. J. A. Sloane.

Lemma 2 *[20] Define*

$$f_1(\tau) = \Theta_{C^\ell}(\tau),$$

where the lattice C^ℓ is as defined in (3). Let $\eta^\ell(\tau) = \Pi_{d|\ell}\eta(d\tau)$ and let $D_\ell = 24, 16, 12, 8, 8, 6, 4, 4, 4, 2$ corresponding to $\ell = 1, 2, 3, 5, 6, 7, 11, 14, 15, 23$. Define

$$f_2(\tau) = \begin{cases} \left(\frac{\eta^\ell(\frac{\tau}{2})\eta^\ell(2\tau)}{\eta^\ell(\tau)^2}\right)^{\frac{D_\ell}{dim\ C^\ell}}, & \ell \text{ is odd;}\\ \left(\frac{\eta^{(\frac{\ell}{2})}(\frac{\tau}{2})\eta^{(\frac{\ell}{2})}(4\tau)}{\eta^{(\frac{\ell}{2})}(\tau)\eta^{(\frac{\ell}{2})}(2\tau)}\right)^{\frac{D_\ell}{dim\ C^\ell}}, & \ell \text{ is even.}\end{cases}$$

The theta series of an ℓ-modular lattice Λ of dimension $k dim(C^{(\ell)})$ can be written as

$$\Theta_\Lambda(\tau) = f_1(\tau)^k \sum_{i=0}^{\lfloor k\ ord_1(f_1)\rfloor} a_i f_2(\tau)^i, \tag{27}$$

where $ord_1(f_1)$ is the divisor of the modular form $f_1(\tau)$, which, in this case, is $\frac{1}{8}\sum_{d|\ell} d$ if ℓ is odd and $\frac{1}{6}\sum_{d|\ell} d$ if ℓ is even.

Let us now take $\ell = 2$. Then $C^2 = \mathbb{Z} \oplus \sqrt{2}\mathbb{Z}$ hence

$$\begin{aligned} f_1(\tau) &= \Theta_{C^2}(\tau)\\ &= \vartheta_3(\tau)\vartheta_3(2\tau)\\ &= 1+2q+2q^2+4q^3+\cdots. \end{aligned} \tag{28}$$

Next, $\mathrm{ord}_1(f_1)$ is computed to be $\frac{1}{2}$. $D_2 = 16$. Finally since 2 is even

$$f_2(\tau) = \left(\frac{\eta(\frac{\tau}{2})\eta(4\tau)}{\eta(\tau)\eta(2\tau)}\right)^{\frac{16}{2}} = \frac{\vartheta_2^2(2\tau)\vartheta_4^2(\tau)}{4\vartheta_3^2(\tau)\vartheta_3^2(2\tau)}.$$

We observe that the denominator of $f_2(\tau)$ is $4f_1^2(\tau)$. We then define a function

$$\begin{aligned} \Delta_4(\tau) &\triangleq f_1^2(\tau) f_2(\tau) \\ &= \tfrac{1}{4}\vartheta_2^2(2\tau)\vartheta_4^2(\tau) \\ &= q - 4q^2 + 4q^3 + \cdots, \end{aligned} \tag{29}$$

and rewrite (27) in the form of (11):

$$\Theta_\Lambda(\tau) = \sum_{i=0}^{\lfloor \frac{k}{2} \rfloor} a_i f_1^{k-2i}(\tau)\Delta_4^i(\tau). \tag{30}$$

For lattices in small dimensions, the first few terms of the theta series can be computed numerically using computer softwares, for example, Magma [29].

Example 5 A generator matrix of the 8-dimensional odd 2-modular lattice in Example 4 can be computed from the generator matrix (26) of the code C:

$$M = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & \sqrt{2} & -1 & -\sqrt{2} \\ 0 & \sqrt{2} & 0 & 0 & 1 & 0 & -1 & -\sqrt{2} \\ 0 & 0 & 1 & 0 & -1 & \sqrt{2} & 0 & \sqrt{2} \\ 0 & 0 & 0 & \sqrt{2} & 1 & -\sqrt{2} & 1 & 0 \\ 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3\sqrt{2} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3\sqrt{2} \end{bmatrix}.$$

To make the typing easy, we compute the Gram matrix

$$MM^T = \begin{bmatrix} 2 & 1 & 0 & -1 & 0 & 2 & -1 & -2 \\ 1 & 2 & -1 & 0 & 1 & 0 & -1 & -2 \\ 0 & -1 & 2 & -1 & -1 & 2 & 0 & 2 \\ -1 & 0 & -1 & 2 & 1 & -2 & 1 & 0 \\ 0 & 1 & -1 & 1 & 3 & 0 & 0 & 0 \\ 2 & 0 & 2 & -2 & 0 & 6 & 0 & 0 \\ -1 & -1 & 0 & 1 & 0 & 0 & 3 & 0 \\ -2 & -2 & 2 & 0 & 0 & 0 & 0 & 6 \end{bmatrix}$$

and input it to Magma to generate the lattice Λ. The first few terms of $\Theta_{\frac{1}{\sqrt{3}}\rho^{-1}(C)}(\tau)$ can be obtained (by the command ThetaSeries(Λ,0,4);):

$$\Theta_{\frac{1}{\sqrt{3}}\rho^{-1}(C)}(q) = 1 + 32q^2 + 128q^3 + 240q^4 + \cdots.$$

Table 2 Weak secrecy gains of odd 2-modular lattices constructed from self-dual codes

dim	theta series	χ_Λ^w
8	$f_1^4 - 8f_1^2\Delta_4$	1.22672
12	$f_1^6 - 12f_1^4\Delta_4$	1.49049
16	$f_1^8 - 16f_1^6\Delta_4$	2.06968
18	$f_1^9 - 18f_1^7\Delta_4 + 18f_1^5\Delta_4^2$	2.35656
20	$f_1^{10} - 20f_1^8\Delta_4 + 40f_1^6\Delta_4^2$	2.70165
22	$f_1^{11} - 22f_1^9\Delta_4 + 66f_1^7\Delta_4^2 - 4f_1^5\Delta_4^3$	3.11161
24	$f_1^{12} - 24f_1^{10}\Delta_4 + 96f_1^8\Delta_4^2 - 28f_1^6\Delta_4^3$	3.60867
26	$f_1^{13} - 26f_1^{11}\Delta_4 + 130f_1^9\Delta_4^2 + -80f_1^7\Delta_4^3$	4.21349
28	$f_1^{14} - 28f_1^{12}\Delta_4 + 168f_1^{10}\Delta_4^2$ $-176f_1^8\Delta_4^3 + 32f_1^6\Delta_4^4$	4.98013
30	$f_1^{15} - 30f_1^{13}\Delta_4 + 210f_1^{11}\Delta_4^2$ $-282f_1^9\Delta_4^3 + 112f_1^7\Delta_4^4$	5.72703

Now in dimension 8, the theta series of a 2-modular lattice can be written as

$$\begin{aligned} &a_0 f_1(\tau)^4 + a_1 f_1(\tau)^2\Delta_4(\tau) + a_2\Delta_4(\tau)^2 \\ &= a_0(1 + 8q + 32q^2 + \cdots) + a_1(q + 0q^2 + \cdots) \\ &\quad + a_2(q^2 + \cdots) \\ &= a_0 + (8a_0 + a_1)q + (32a_0 + 0 + a_2)q^2 + \cdots . \end{aligned} \tag{31}$$

We then have three linear equations in three unknowns a_0, a_1 and a_2

$$\begin{cases} a_0 = 1 \\ 8a_0 + a_1 = 0 \\ 32a_0 + a_2 = 32, \end{cases}$$

which gives $a_0 = 1$, $a_1 = -8$ and $a_2 = 0$, yielding the theta series

$$\Theta_{\frac{1}{\sqrt{3}}\rho^{-1}(C)}(q) = f_1(\tau)^4 - 8f_1(\tau)^2\Delta_4(\tau). \tag{32}$$

Theta series of the twelve odd 2-modular lattices constructed in [24] are computed and shown in Table 2, as polynomials in f_1 and Δ_4 for simplicity. Their weak secrecy gains are approximated using Mathematica [27].

4 Best known lattices

Now that we have computed the weak secrecy gains of several 2- and 3-modular lattices, we want to compare them with the best unimodular lattices in their respective dimensions. Figure 2 compares the secrecy gains of the best unimodular lattices with the weak secrecy gains of the 2- and 3-modular lattices we have computed. We can see that most of these even 2- and 3-modular lattices, indicated by disconnected big dots, outperform the unimodular lattices except in dimension 22, and three of the odd 2-modular lattices, indicated by disconnected small dots, outperform the unimodular lattices, in particular, in

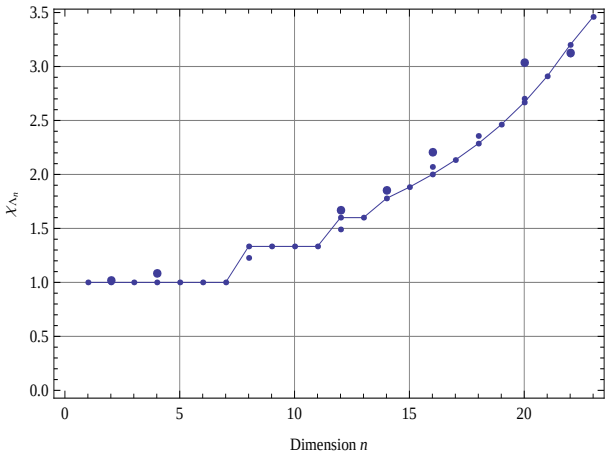

Fig. 2 The weak secrecy gain of 2- and 3-modular lattices vs. unimodular lattices as a function of the dimension n

Table 3 List of 2- and 3-modular lattices out-performing the best unimodular lattices

dim	lattice	ℓ	χ_Λ
2	$\mathbb{Z}^2$	1	1
2	A_2	3	≥ 1.01789
4	$\mathbb{Z}^4$	1	1
4	D_4	2	≥ 1.08356
12	D_{12}^+	1	1.6
12	K_{12}	3	≥ 1.66839
14	$(E_7^2)^+$	1	1.77778
14	$C_2 \times G(2,3)$	3	≥ 1.85262
16	$(D_8^2)^+$	1	2
16	$\frac{1}{\sqrt{3}}\rho^{-1}(C)_{real}$	2	≥ 2.06968
16	BW_{16}	2	≥ 2.20564
18	$(D_6^3)^+$ or $(A_9^2)^+$	1	2.28571
18	$\frac{1}{\sqrt{3}}\rho^{-1}(C)_{real}$	2	≥ 2.35656
20	$(A_5^4)^+$	1	2.66667
20	$\frac{1}{\sqrt{3}}\rho^{-1}(C)_{real}$	2	≥ 2.70165
20	HS_{20}	2	≥ 3.03551
22	$(A_1^{22})^+$	1	3.2
22	$A_2 \times A_{11}$	3	≥ 3.12527

dimension 18, the odd 2-modular lattice has the best secrecy gain known by now.

Table 3 gives a list of 2- and 3-modular lattices out-performing the best unimodular lattices.

5 Conclusion and future work

This paper computes the weak secrecy gains of several known 2- and 3-modular lattices in small dimensions. Most of the even 2- and 3-modular lattices and three of the odd 2-modular lattices have a higher secrecy gain than the best unimodular lattices. We then conclude that, at least in dimensions up to 23, 2- and 3-modular lattices are better option for Gaussian wiretap channel.

A line of future work would naturally be investigating ℓ-modular lattices for other values of ℓ to understand if bigger ℓ allows better modular lattices in terms of secrecy gain. Also, more 2- and 3-modular lattice examples should be found to get a better understanding of why they have a higher secrecy gain, since a classification of such lattices is currently unavailable even in small dimensions.

Acknowledgment

The research of F. Lin and of F. Oggier for this work is supported by the Singapore National Research Foundation under the Research Grant NRF-RF2009-07. The research of P. Solé for this work is supported by Merlion project 1.02.10.

The authors would like to thank Christine Bachoc for helpful discussions.

References

1. F. Lin and F. Oggier, "A Classification of Unimodular Lattice Wiretap Codes in Small Dimensions", to appear in *IEEE Trans. Inf. Theory*.
2. A. D. Wyner, "The wire-tap channel," Bell. Syst. Tech. Journal, vol. 54, October 1975.
3. Y. Liang, H.V. Poor and S. Shamai, "Information theoretic security," Foundations and Trends in Communications and Information Theory, Vol. 5, Issue 4-5, 2009, Now Publishers.
4. L. H. Ozarow and A. D. Wyner,"Wire-tap channel II," *Bell Syst. Tech. Journal*, vol. 63, no. 10, pp. 2135-2157, Dec. 1984.
5. A. Thangaraj, S. Dihidar, A. R. Calderbank, S.W. McLaughlin, and J.-M. Merolla,"Applications of LDPC Codes to the Wiretap Channel," *IEEE Trans. Inf. Theory*, vol. 53, No. 8, Aug. 2007.
6. Hessam Mahdavifar and Alexander Vardy, "Achieving the Secrecy Capacity of Wiretap Channels Using Polar Codes," *IEEE Trans. Inf. Theory*, vol.57, no. 10, pp. 6428-6443, Oct. 2011.
7. S.S. Ong and F. Oggier, "Lattices from Totally Real Number Fields with Large Regulator", International Workshop on Coding and Cryptography (WCC 2013), Bergen.
8. S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel", *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451-456, July 1978.
9. D. Klinc, J. Ha, S. McLaughlin, J. Barros, and B. Kwak, "LDPC codes for the Gaussian wiretap channel," in *Proc. ITW*, Oct. 2009.
10. R. Liu, H.V. Poor, P. Spasojevic, and Y. Liang, "Nested codes for secure transmission", in Proc. PIMRC, 2008, pp.1-5.
11. J.-C. Belfiore and F. Oggier, "Secrecy gain: a wiretap lattice code design," ISITA 2010. `http://arXiv:1004.4075v2` [cs.IT].
12. C. Ling, L. Luzzi, J.-C. Belfiore, "Semantically Secure Lattice Codes for the Gaussian Wiretap Channel", `http://arXiv:1210.6673` [cs.IT].

13. J.-C. Belfiore and P. Solé, "Unimodular lattices for the Gaussian Wiretap Channel," ITW 2010, Dublin. http://arXiv:1007.0449v1 [cs.IT].
14. F. Oggier, J.-C. Belfiore, and P. Solé, "Lattice Coding for the Wiretap Gaussian Channel", http://arXiv:1103.4086v1 [cs.IT], 21 Mar 2011.
15. A.-M. Ernvall-Hytönen, "On a Conjecture by Belfiore and Solé on some Lattices", to appear at *IEEE Transactions on Information Theory*.
16. A.-M. Ernvall-Hytönen, "A Short Note on the Kissing Number of the Lattice in Gaussian Wiretap Coding," http://arXiv:1209.3573 [cs.CR], 17 Sep 2012.
17. F. Lin and F. Oggier, "Gaussian Wiretap Lattice Codes from Binary Self-dual Codes," *2012 IEEE Information Theory Workshop (ITW)* pp. 662-666.
18. Fuchun Lin and Frederique Oggier, "Secrecy Gain of Gaussian Wiretap Codes from 2- and 3-modular Lattices," *2012 IEEE International Symposium on Information Theory (ISIT)* pp. 1747-1751.
19. H.-G. Quebbemann, "Modular Lattices in Euclidean Spaces," Journal of Number Theory 54 (1995), 190-202.
20. E.M. Rains and N.J.A. Sloane, "The Shadow Theory of Modular and Unimodular Lattices," J. Number Theory, 73 (1998), 359-389.
21. F. J. MacWilliams and N. J. A. Sloane, "The Theory of Error-Correcting Codes", Amsterdam, The Netherlands: North-Holland, 1977.
22. I.N. Stewart and D.O. Tall, "Algebraic Number Theory," Chapman and Hall, 1979.
23. Christine Bachoc, "Applications of Coding Theory to the Construction of Modular Lattices," Journal of Combinatorial Theory, Series A 78, 92-119, 1997.
24. Robin Chapman, Steven T. Dougherty, Philippe gaborit and Patrick Solé, "2-modular Lattices from Ternary Codes," *Journal de Théorie des Nombres de Bordeaux*, tome 14, n^0 1, 2002, pp. 73-85.
25. N. Koblitz, "Introduction to Elliptic Curves and Modular Forms", Graduate Texts in Math. No. 97, Springer-Verlag, New York, Second edition, 1993.
26. T.M. Apostol, Introduction to Analytic Number Theory, Springer-Verlag, 1976.
27. Wolfram Research, Inc., Mathematica, Version 8.0, Champaign, IL (2010).
28. http://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/
29. http://magma.maths.usyd.edu.au/magma/